CRYPTO: IS IT TOO MUCH PROTECTION?

by

Walker W. Watson

Presented to Webster University in Partial Fulfillment
of the Requirements for the Master of Arts Degree

Professor Thomas F. Brown
SMG 508 - Information Systems Security

September 29, 1993

CRACKERS V.S. HACKERS R. U. Sirius: "Once there were computer hackers. These early pioneers of computing were fanatically dedicated to inventing and exploring how things worked. As part of the sixties generation, they were also prone toward being anti-establishment and somewhat disrespectful toward property rights. 'The early hackers were fond of breaking bureaucratic laws and regulations, particularly if they got in the way of learning something or doing something useful." (Sirius, p 54) Two of the early hackers, Steve Wozniak and Steven Jobs, in their garage, put together the first successful commercial personal computer. This evolution caused a flood of hackers to flow into the industry, many of them becoming rich and gaining positions of authority. "Most of them maintained a semblance of their early anti-bureaucratic attitudes but generally settled down to the task of creating the information/communications ecology that now dominates Western life." (Sirius, p.54)

"Meanwhile two things happened. 1) A new generation of hackers emerged who were not yet part of the establishment. Like their predecessors, they were inventive, curious, and too smart to buy into dumb laws and bureaucratic regulations. As the earlier hackers were influenced by the idealism of the hippie and new-left movements, the new-generation hackers were influenced by the nihilism and alienation of the punk movement. 2) The world economic and social order went completely digital. And so CRIME went digital too." (Sirius, p. 54)

Between the new generation of alienated young hackers and the world of organized crime emerges the concept of a cracker. This term is a result partially of the older-generation hackers trying to separate themselves from computer crime. Debate still rages over exactly what constitutes the difference between hacking and cracking. "Some say that cracking represents any and all forms of rule-breaking and

illegal activity using a computer. Others would define cracking only as as particularly DESTRUCTIVE criminal acts. Still others would claim that the early hackers were EXPLICITLY anarchistic and that acts of willful destruction against a "the system" have a place in the hacker ethos, and that, therefore, the term cracker is unnecessary and insulting." (Sirius, p. 54)

INFORMATION THEFT "Information can't be stolen. Unless they've come up with something new, phenomnologically speaking." (Synergy, p. 54) If a person knows something, and tells someone else, they still know what they told. Property laws were set up to handle tangible objects. We're dealing with raw data, information. "The whole system to handle "ownership" is obsolete. In a world where you can copy information, leaving the original intact, and wind up with the perfect copy, the debate over ownership is over." (Synergy, p. 54)

ON MONEY AND COMPUTER CRIME As Michael Synergy points out, Richard Nixon was our most important president. He took the country off the gold standard. Until then, "...money in the bank had to be related to a real-world object. But suddenly the governor was removed. Money was just a bunch of bits and bytes in computers. Money became the first exploration into cyberspace." (Synergy, p. 55) Mr. Synergy goes on to make the observation that "This is why the economy is messed up. This is why banks are messed up. This is why computer crime is growing exponentially." (Synergy, p. 55) As a result of the move to digital money the damage caused electronically can be significant. The reason for this, as Mr. Synergy says, is that, "We've stopped using reality as the "acid test" for what was represented in our machines." (Synergy, p. 55)

As society becomes more digital, it will become easier to change completely the way we deal with money. Changing a document, changing a date, changing a "no" to a "yes", or adding figures to a bank balance, all this becomes very simple through the

use of computers, "How do you trace things like that? If you're a good programmer, there are no fingerprints." (Synergy, p. 55)

CRACKING THE BANK Take for example the Automated Teller Machines that every bank in business today, and bank customers use with fanatical frequency. " The Banking industry has acted with almost criminal negligence when it comes to the security of their customers' ATM accounts. The industry's apparent nonchalance betrays a level of stupidity, at the highest levels of bank security, undreamt of by the average patron." (Russell, p. 56)

Russell points out that the banks have created a system that is vulnerable to substantial losses. This is especially true in the way the ATM data is processed at the various off-site locations, such as grocery stores, and gas stations. "If you use an ATM card, your bank account is particularly vulnerable at such terminals...And all ATMs are sitting ducks for the dedicated cybercracker." (Russell, p.55)

The track data follows for a withdrawal provides an observation of the fatal flaws. Customers insert their card and enter their "secret code", usually four to six characters long. This information is sent over a phone line by modem to the bank computer. The computer checks the card number and the PIN code. If a match is made, the machine asks for the amount of cash desired, or authorizes the purchase and sends the transaction details back to the central computer. "All this takes place through standard modem protocol with no attempt, at present, to encrypt the important details. Banks, while using more secure dedicated phone lines for their own ATM machines, have allowed many "convenience" locations for twenty-four-hour fast cash to spring up without making even a perfunctory bow toward security," (Russell, p. 55) The gas stations and grocery stores with ATM services are easy targets for computer crackers to tap. If you use an ATM at any of these locations, you account information is available, just for the asking.

In light of several ATM heists and conspiracies the banks and ATM companies "...appear to be taking protective measures," (Russell, p. 58) Some of the larger companies have said they are making sure their contractors follow procedures to protect secret account information. "...yet while these financial groups are protecting data from people on the inside, any enterprising cyberpunk on the outside can knock off ATMs at any of 72,000 convenient locations twenty-four hours a day. Sleep well, citizens..." (Russell, p. 55)

Average customers don't bear the loss of the criminal actions. They are reimbursed for any changes to their accounts. Banks, eager to avoid bad publicity, and customer paranoia are quick to cover losses. "This of course, is the final detail which will send the wavering cyberpunk..." Russell, p. 58) to the nearest ATM!

Criminal prosecution has done little to stem the tide. Court transcripts and newspaper accounts widely spread the information. While banks rush to change their security measures, cyberpunks develop even more sophisticated tools for their armories. While "there's nothing the average Joe can do but to become a Luddite or refill his Valium prescription." (Russell, p.59) some protective measures can be taken by the authorities.

SAFE COMMUNICATIONS "Telecommunications security is a source of increasing concern for individuals, corporations, and governments. As the flow of information...increases, so does the likelihood of exposure to the wrong parties." (Wade, p. 15A) The amount of information exchanged over unsecured channels for efficiency and productivity is increasing at an astounding rate. As this volume grows, the nature and the sensitivity of the data rises as well.

Today business people can't wait to meet with another person to exchange data, or they can't afford delays when data is carried by traditional physical transportation modes. But when using electronic channels to transmit important

business information and data are they asking the question, "Can I afford to lose the confidentiality of the information?" (Wade, p. 15A)

As Mr. Wade points out, competition worldwide is heating up. Former spy agencies, like the KGB, have openly stated they are going into industrial espionage as a replacement for the loss of old fashioned political spy business. "U.S. intellectual property, new product research, and future marketing programs are becoming a gold mine..." (Wade, p. 15A) just wating to be tapped.

Recent surveys show that 60% of daily business communications moves over telephone lines. Much information that is sensitive, and proprietary is transmitted by voice, fax and computers via microwave, satellite and fiber-optic links.

"The alternative to limiting information sent over telecommunications media...is to protect the information from end to end." (Wade, p. 15A) Security managers, through the creation of procedures for encryption of data, can close some of the potential loopholes of loss. "Cryptography has proven to be highly effective against wiretapping and monitoring public and private networks." (Wade, p. 15A)

CLIPPER: SECURITY V.S. PRIVACY As a measure of even more privacy and protection for business communications, the Clinton administration this spring endorsed a new technology called the Clipper chip, for data encryption. Encryption of data is a long established means of communications security. As the government endorses this technology naturally law-enforcement and privacy advocates are rounding up their wagons to stake out positions that will likely test the bounds of the Constitution.

The Clipper chip is an electronic apparatus that can be incorporated directly into the design of computerized hardware such as telephones, computers and other communications devices. The chip has, on board, a sophisticated encryption formula called an algorithm that protects a company's communications by scrambling the

data.

The Clipper chip is a joint development of the National Security Administration (NSA) and the National Institute for Standards and Technology (NIST). Its purpose is to become a balance between the privacy needs of business and law-enforcement. "The Clinton administration is encouraging American businesses to adopt Clipper to ensure their own privacy, yet still permit 'lawful government electronic surveillance,' according to a statement released by the White House." (Schwartau, p. 207)

There are two keys to the device that permit decoding of encrypted messages. These two keys are to be held, according to the government, by two independent parties, such as the Federal Reserve Board and a private company. Recently the government has delayed its announcement of the key holders until later this year.

The Clipper technology and its encouragement by the government comes from Bush era intelligence-agency attempts to provide, through legislation, a back door to encrypted communications. The EFF (Electronic Frontier Foundation) and CPSR (Computer Professionals for Social Responsibility) were successful in having such riders removed from legislative bills.

Among anti-Clipper privacy advocates there are deep concerns, especially on the integrity of who will hold the decoding keys to the U.S. information kingdom. Some believe, like so many other secrets, this too will leak out. As a result of their concerns, few businesses have lined up to adopt and work with the government's plan. A consortium of 31 major companies sent a letter to the White House and Congress stating, "...We believe that there are fundamental privacy and other constitutional rights that must be taken into account when any domestic surveillance is proposed." (Schwartau, p. 207)

Despite conventional cryptological wisdom which says that only after

widespread public analysis and comment should an encryption technique be trusted, the government has stated their intention to keep all Clipper technical information secret. As a result CPSR filed a lawsuit against NSA and the National Security Council seeking information about Clipper. As Mr. Schwartau, points out,

> "The Clipper plan was developed behind a veil of secrecy...We need to know why the standard was developed, what alternatives were considered and what the impact will be on privacy. As the proposal currently stands, Clipper looks a lot like desktop surveillance." (p. 207)

Another stance by Mitch Kapor, the founder of Lotus Development Corporation and the chairman of the EFF, as quoted by Mr. Schwartau is, "An [encryption] system based upon classified, secret technology will not and should not gain the confidence of the American public." (p. 215)

The majority of business leaders think that the voluntary adoption of Clipper "is only the first step in a plan drawn by the intelligence community years ago that will mandate Clipper encryption for private business." (Schwartau, p. 215) The Electronic Frontier Foundation, the American Civil Liberties Union, the Computer Professionals for Social Responsibility and other like groups are making sure that the government never gets that far.

Some considerations American businesses must make before adopting Clipper encryption technology into their communications are:

the algorithm is good enough to prevent decoding,

the government doesn't have its own back door to read Clipper messages,

the key-escrow agents are trustworthy,

can the key repository withstand a direct attack,

by using Clipper the company is not giving up its rights to privacy,

hardware using Clipper is better than current encryption technology.

The argument in response to negative attitudes about Clipper from the government has been "while [other forms of] encryption technology can help Americans protect business secrets and the unauthorized release of personal information, [they] also can be used by terrorists, drug dealers, and other criminals." (Schwartau, p. 215) Some believe Clipper is good enough, they are in the minority. Most businessmen hold the majority opinion that, while Clipper may be what the government wants, it shouldn't consider creating laws that make Clipper use mandatory.

CAPTAIN CRUNCH SPEAKS OUT Wes Thomas, in an interview with John Draper, also known as Captain Crunch, the prototypical phone phreak, who switched sides to law and order, asks, "What do you think of the Clinton administration's proposed Clipper chip for encrypting phone calls? And registering everyone's encryption keys to provide tappibility in criminal investigations?" (Thomas, p. 42)

Captain Crunch, a.k.a. John Draper, replies, "I believe they're trying to push this idea through without giving much thought to the ramifications. This overwhelming urge to tap into our private conversations is simply going to promote private encryption and voice scrambling." (Thomas, p. 42) He goes on to say, that it won't make law enforcements job any easier, because, would a criminal register his phone with the government? And would law abiding citizens entrust the government to safeguard their encryption key?

Mr. Thomas asks, "What's the reaction so far?" (Thomas, p. 42) "Very negative. This is not only going to get a bad reception in the industry, but it will cost the government more money by piling on huge administrative costs." (Thomas, p. 44) He continues with a question that has been asked before, is there a governmental agency that can be trusted to keep track of the key? How will the government keep track of the possibly millions of public keys for Clipper devices sold? What if someone

wants to sell their device? The question is raised again, will it be impossible to be sure that there isn't a back door to the algorithm used in the chip?

Captain Crunch observes that, "Its clear that the industry hasn't been consulted, or the idea put forth in some public forum. So, where is the democratic process? How was this company that sells the Clipper chip selected? Were RSA data security people contacted? A lot of questions will have to be answered before something like this can be accepted." (Thomas, p. 44)

WHAT YOU DON'T KNOW CAN HURT YOU Dundee Friedman, writing on the same subject, the Clipper controversy, states, "Encryption is not yet widespread, but soon will be. So the White House comes out and says 'we'll protect you,' conveniently failing to mention that perfectly good encryption devices are already available. What perfectly good means to me is that the government can NOT listen whenever they want." (Friedman, p. 42)

When the DES (Digital Encryption Standard) algorithm was announced, everyone wondered if it had a back door. That is, a method or property that would allow someone who wanted to know to read anything inside the DES envelope. The NSA with the Clipper "...has gotten bolder, folks. This wiretap chip [Clipper], whose actual algorithm is secret, is designed to be compromised, and that's not a bug but a feature," (Fiedman, p. 42)

To get the process started the Department of Justice will purchase 2000 telephones with the Clipper chip in them. They are going to use civil forfeiture funds to pay for them. "Its got that great spook logic to it: make the criminals pay for their own surveillance. Except that you don't have to be convicted to pay forfeit, and nobody is mandating the use of these devices–not yet." (Fiedman, p. 43)

Next the plan will call for prevention of other devices being sold. Then, the use of non-wiretap encryption will become illegal. "If you can't decrypt something for

them, you lose. Use a random number, go to jail." (Fiedman, p. 43)

What can the average Joe computer/telecommunications user do to prevent this outrage? First, tell everyone you know about this wiretap fiasco. Write your Congressman, let him know this is a voting issue. Send e-mail to the White House protesting the use and endorsement of the Clipper chip and any other similar scheme to protect our privacy. "But best if all, START USING ENCRYPTION. Ask your suppliers of software and telephones for cryptographic privacy." (Fiedman, p. 43) Most of all, don't buy Clipper products or any of its successors.

Finally, just keep in mind what Friedman ends with: "When the thought police come, it will be because of what you told your mother, or your lover, or your doctor, or your shrink, or your accountant." (Friedman, p. 43)

REFERENCES

Friedman, Dundee "Use a random number, go to jail." *MONDO 2000*, Issue No. 10, 1993

Russell, Morgan "The ATM Crack: Terminal Disorders." *MONDO 2000, Users Guide to the New Edge*, HarperPerennial, New York, NY, 1992

Schwartau, W. "Crypto policy and business privacy." *PC Week*, June 28, 1993

Sirius, R.U. "Crackers." *MONDO 2000, Users Guide to the New Edge*, HarperPerennial, New York, NY, 1992

Synergy, Michael "On Theft of Information." *MONDO 2000, Users Guide to the New Edge*, HarperPerennial, New York, NY, 1992

Thomas, Wes "Captain Crunch, Whistle Blower: A report from the Front Lines." *MONDO 2000*, Issue No. 10, 1993

Wade, Bob "Encryption: A Primer." *Security Management*, March, 1993